Exhibit A

IN THE HIGH COURT OF JUSTICE
BUSINESS AND PROPERTY COURTS
OF ENGLAND AND WALES
BUSINESS LIST (ChD)

Case No. HC-2016-002798

Assigned to: THE HON MR JUSTICE MICHAEL GREEN

BETWEEN:

RAS AL KHAIMAH INVESTMENT AUTHORITY

Claimant and Defendant to Counterclaim

-and-

FARHAD AZIMA

Defendant and Counterclaimant

-and-

STUART PAGE

First Additional Defendant to Counterclaim

-and-

DAVID NEIL GERRARD

Second Additional Defendant to Counterclaim

-and-

DECHERT LLP

Third Additional Defendant to Counterclaim

-and-

JAMES EDWARD DENISTON BUCHANAN

Fourth Additional Defendant to Counterclaim

***Draft* AMENDED COUNTERCLAIM AND**

CLAIM AGAINST ADDITIONAL PARTIES

As the counterclaim has been remitted for a fresh trial taking account of further evidence, and is also brought against further parties, this pleading sets out the case afresh, as follows.

I. THE PARTIES

1. The Counterclaimant, Mr Azima, is a businessman and US citizen with many decades of experience in the aviation industry.

2. The Defendant to the Counterclaim ('**RAKIA'**) is the investment authority of the Emirate of Ras Al Khaimah ('**RAK**'), which is one of the seven Emirates that comprise the United Arab Emirates. Mr Azima has had commercial dealings with RAKIA over several years.

3. In addition to RAKIA, Mr Azima brings this Counterclaim against four further defendants (the '**Additional Defendants**') as follows:

   a. Mr Stuart Page is an investigator. He operates in the Middle East and other jurisdictions. Mr Page was RAKIA's agent at all material times.

   b. Mr Neil Gerrard is a solicitor. In 2014 he was engaged by RAKIA.

   c. Dechert LLP ('**Dechert'**) is the law firm in which Mr Gerrard was a partner until late 2020. Dechert is liable for the acts and omissions of Mr Gerrard pleaded below.

   d. Mr James Buchanan was employed by RAK Development LLC from September 2014 following an introduction by Mr Gerrard. From November 2014, Mr Buchanan was authorised by RAKIA to undertake various activities on its behalf.

   e. RAKIA is primarily and/or vicariously liable for the acts and omissions of the Additional Defendants pleaded below and/or has ratified them. RAKIA and the Additional Defendants are jointly responsible for the wrongs set out below.

4. The Defendants and others have sought to conceal the matters complained of and the true facts continue to emerge. Mr Azima's right later to seek to join further parties shown to be responsible for the events described below is reserved.

II. BACKGROUND AND PROCEDURAL CONTEXT

5. Between 2015 and 2016, Mr Azima's computers and email accounts were unlawfully hacked, without his knowledge or authority.

6. Approximately 30GB of Mr Azima's private and confidential data was released on to the internet in August and September 2016 ("**the hacked data**"). Additional leaks to Mr Azima's private and confidential data were subsequently published including in 2017 and 2019.

7. RAKIA brought proceedings against Mr Azima in tort in September 2016, alleging fraud and conspiracy; relying on documents and information extracted from the hacked data.

8. Mr Azima alleged amongst other things that RAKIA was responsible for hacking his emails and other documents and for related wrongdoing including the publication of his data online, and brought a counterclaim against RAKIA.

9. RAKIA claimed to have discovered the hacked material on publicly available sources on the internet.

10. Following a trial ('**the First Trial**'):

    a. various of RAKIA's claims were upheld and RAKIA was awarded damages, pre-judgment interest and costs;

    b. it was found that RAKIA's responsibility for the hacking had not been established and the counterclaim was dismissed.

11. Mr Azima appealed. By its order made on 15 March 2021, the Court of Appeal:

    a. set aside the dismissal of the counterclaim and ordered that the hacking issue was to be remitted for a further trial;

    b. directed that the findings made on the hacking issue were not to be binding in the remitted trial;

    c. ordered that in the event that Mr Azima succeeded on the hacking issue in the remitted trial, the orders made as to costs and interest were to be set aside and would be in the discretion of the judge hearing the remitted trial;

d. granted two applications made by Mr Azima to admit new evidence relating to the hacking issue;

e. held that even if Mr Azima succeeds in establishing that RAKIA was responsible for the hacking, its claims should not be struck out and the evidence so obtained should not be excluded.

12. Mr Azima has sought permission from the Supreme Court to appeal against (i) the latter of those findings; (ii) the rejection of his defence of set-off; and (iii) the dismissal of his appeal against one of RAKIA's claims. If permission to appeal is granted and the appeal is allowed, Mr Azima will rely on the hacking in defence of RAKIA's claims and will amend this counterclaim as appropriate.

13. Mr Azima brings this counterclaim in accordance with the Court of Appeal's judgment and Order, adding the Additional Defendants on the basis that they are jointly and severally liable for the hacking and related wrongs.

14. The hacking was covert, and RAKIA and the Additional Defendants have conspired to cover up and conceal the true facts. The facts have emerged over time, including in the stages summarised below, and continue to emerge.

15. The facts known by the opening of the First Trial included:

a. In around 2014, RAKIA was in a bitter dispute with its former CEO, Dr Khater Massaad.

b. By around March 2015, RAKIA had identified that Mr Azima was working with Dr Massaad, managing a "*team*" in the US working to draw attention to allegations of human rights abuses in RAK; and a "Project Update" Report proposed action against Mr Azima and his team, including steps to "*gather intelligence on their progress in order to monitor their activities and attempt to contain or ruin their plans*".

c. Shortly after the Project Update, the Ruler of RAK (HH Sheikh Saud bin Saqr Al Qasimi, ('**the Ruler**')) gave instructions to Mr Buchanan and other advisers to "*target*" and "*go after*" Mr Azima.

d. In around October 2015, unauthorised access was obtained to one of Mr Azima's email accounts; and another account was accessed in 2015 and early 2016 from India and Bulgaria (where Mr Azima had not been present).

e. In late December 2015, a RAKIA document sent to Mr Gerrard stated that "*through a series of investigations*" it had been "*established as fact*" that Mr Azima had "*orchestrated*" certain frauds.

f. In July 2016, Mr Gerrard told Mr Azima at a meeting between them and Mr Buchanan that if Dr Massaad did not agree to a settlement of his dispute, Mr Azima would be rendered "*collateral damage*."

g. The dispute was not settled and within weeks, over 30GB of Mr Azima's confidential and/or private data were placed online on torrent sites (the '**Torrents**') in three tranches.

16. During the First Trial it emerged amongst other things that:

a. The Project Update had been provided by Mr Page, and his denials in his witness statement that he had provided any written briefings or had any knowledge of Mr Azima in 2015 were false and dishonest.

b. Mr Gerrard, Mr Buchanan and the Ruler had provided witness statements which deliberately minimised Mr Page's role and the Project Update.

c. Mr Buchanan gave evidence that his knowledge of Mr Azima's allegedly fraudulent conduct had been derived from sight of the hacked materials.

d. As a matter of law and/or by inference, it followed that RAKIA's knowledge of Mr Azima's allegedly fraudulent conduct had been derived from sight of the hacked materials.

e. RAKIA's account that it had 'discovered' the hacked materials on websites through Mr Page and an associate, Mr Halabi, was false and dishonest.

17. Shortly after Judgment was handed down:

a. Mr Gerrard notified the Court that there were 'inaccuracies' in the evidence he had given under cross-examination during the trial concerning his interrogations of the former general counsel of RAKIA, Mr Karam Al Sadeq.

b. Mr Gerrard served a 'corrective' witness statement showing that his evidence had been materially wrong; but did not satisfactorily explain how he had come to give 'inaccurate' evidence or the delay in correcting it.

18. Following the First Trial, searches located more than 150 surviving 'spear-phishing' emails received by Mr Azima and others associated with him in 2015 immediately after the Project Update and in the months following, which:

    a. had common features including timing, recipients, the use of common spoofed sender accounts and content, and the inclusion of false content tailored specifically to the recipients;

    b. pointed to a single 'spear-phishing' campaign targeting Mr Azima and associated persons.

19. A witness statement of an investigator, Mr Jonas Rey, records that he was informed by an unidentified source in India that from about October 2014, multiple firms in India had been approached by Mr Page to hack Mr Azima.

20. Bank statements of an Indian firm, CyberRoot Risk Advisory Private Limited ('**CyberRoot**') were revealed in other proceedings in late January 2021:

    a. Which show that over $1m had been paid to it between 2015 and 2017 by a company (Vital Management Services - '**Vital'**) controlled by Mr Nicholas Del Rosso;

    b. At least a material part of which relate to work for RAKIA on the instructions of Mr Gerrard and/or Dechert.

21. It has subsequently been revealed that the bank statements also show substantial payments to CyberRoot by Gravitas International LLC ('**Gravitas'**), an enterprise owned and controlled by Mr Buchanan.

22. A former CyberRoot employee has admitted to Mr Rey:

    a. that he and others at CyberRoot had hacked Mr Azima's computers and emails;

    b. that he did so on the instructions of Vital, in turn taking instructions from Dechert, on RAKIA's behalf.

23. In early 2020, Mr Al Sadeq brought proceedings against Mr Gerrard, Dechert, and two other solicitors at Dechert (Mr David Hughes and Ms Caroline Black), alleging that he was mistreated and tortured while in custody in RAK and that they participated in and are liable for this abuse. In those proceedings:

a. Mr Al Sadeq's solicitors are Stokoe Partnership ('**Stokoe**').

b. Stokoe obtained *Norwich Pharmacal* relief in regard to attempts to hack its systems and obtain its confidential information, and Mr Patrick Grayson was identified as having given instructions for those activities and having himself received instructions from and worked closely with Mr Del Rosso.

24. Mr Grayson (working for GPW, a company associated with him) also provided services to RAKIA in regard to the RAK Project, but his involvement was not disclosed by RAKIA when it was ordered in 2018 to identify the investigative entities that it engaged. The nature of those services remains under investigation, and Mr Azima reserves the right to apply to join Mr Grayson as a defendant if it emerges that he was party to the hacking or other wrongdoing against Mr Azima alleged herein.

25. Mr Page has also been sued by Stokoe, and in August / September 2020 told Mr Buchanan that "*if I have to implicate Nick / Patrick, Decherts, Neil and the boss to get me out of this I will*" (referring to Mr Del Rosso, Mr Grayson, Dechert, Mr Gerrard and the Ruler).

26. Mr Azima reserves the right to develop or amend his case as further information comes to light.

III. THE HACKING

A. THE "RAK PROJECT"

27. Dr Khater Massaad was the CEO of RAKIA for several years until 2012. A dispute developed between Dr Massaad and RAKIA in which:

a. Dr Massaad asserted that RAKIA owed him substantial sums in connection with his service as CEO, and

b. RAKIA claimed that Dr Massaad had been responsible for mismanagement and wrongdoing including embezzlement.

28. RAKIA sought to obtain information about Dr Massaad and persons whom it perceived to be associated with him, including Mr Azima.

29. These activities were at times referred to by individuals on RAKIA's side as the "RAK Project".

B. RAKIA'S AGENTS

30. In connection with its disputes with Dr Massaad and persons whom it perceived to be associated with him, including Mr Azima, RAKIA engaged Dechert LLP, and its partners Mr Gerrard and Mr David Hughes to act on its behalf.

31. RAKIA, directly or through Dechert LLP, engaged investigators and other persons and entities, to investigate and gather information from and about Dr Massaad and persons whom it perceived to be associated with him, including, Mr Azima. The persons and entities engaged included:

    a. Mr Page (and companies controlled by him, including Stuart Page MEFZ);

    b. Mr Del Rosso (and Vital);

    c. Karv Communications ('**Karv**'), whose employees included Mr Andrew Frank and Mr Amir Handjani;

    d. Mr Patrick Grayson (and GPW).

32. At all material times from late 2014, Mr Buchanan:

    a. was employed by RAK Development LLC, to manage certain of RAKIA's affairs; and

    b. had authority to take steps on RAKIA's behalf pursuant to a power of attorney.

33. On behalf of RAKIA, channels of communication used in relation to the RAK Project and the wrongs set out below included:

    a. Mr Buchanan providing instructions to Mr Gerrard;

    b. Mr Gerrard providing instructions to Mr Del Rosso and Vital; and

    c. Mr Buchanan and Mr Gerrard providing instructions to Mr Page and his companies.

34. The Additional Defendants, Mr Del Rosso and Mr Grayson (and their companies) were at all material times agents or servants of RAKIA, and:

a. their knowledge and conduct in connection with the "RAK Project" is attributable to RAKIA, which is thus primarily liable;

b. RAKIA is vicariously liable for their acts or omissions; and/or

c. RAKIA has ratified their acts or omissions.

1. Mr Page

35. Mr Page:

a. was engaged by RAKIA to perform investigatory and related work on the RAK Project;

b. provided briefings and reports on the RAK Project approximately once a month;

c. adopted with RAKIA an intentional policy of destroying the written reports after each briefing with the intention of keeping their contents secret;

d. received very substantial remuneration of at least $100,000 per month; from which it is to be inferred that the services he provided were either very substantial or risky.

36. Mr Page has been implicated in or connected to hacking and other wrongdoing in other proceedings:

a. In *Dubai Aluminium v Al Alawi* [1998] EWHC 1202 (Comm), it was found that a sub-agent engaged by Mr Page obtained confidential information using illegal pretext calls.

b. Mr Page was engaged by the Board of Control for Cricket in India to investigate several board members and players in 2013-2014. Following that appointment, confidential emails passing between individuals the subject of the inquiry were circulated to the media.

c. In *JSC BTA Bank v Ablyazov* [2018] EWHC 259 (Comm), it was found that the claimant bank was contacted in early 2016 by Mr Page, claiming to act for unnamed Israeli hackers who had extracted information from a computer belonging to a Mr Aggarwal, an accountant, and seeking to find out whether the bank was interested in obtaining the information.

d. In *Re Al M* [2019] EWHC 3415 (Fam) it was found that serious criminal conduct had been undertaken by someone acting for the Ruler of Dubai, later identified by Court order on 28 September 2020 as Mr Page.

37. A witness statement of an investigator, Mr Rey, records that he was informed by an unidentified source in India that from about October 2014, multiple firms in India had been approached by Mr Page to hack Mr Azima.

38. It is to be inferred that Mr Page:

a. has connections with and access to hackers;

b. has worked with hackers;

c. is prepared to undertake serious wrongdoing on behalf of his clients.

2. Mr Del Rosso

39. Mr Del Rosso and Vital:

a. Acted on behalf of RAKIA in obtaining services from CyberRoot at a cost which indicates that the services were unusual or very substantial;

b. Acted on behalf of RAKIA in arranging for the download of hacked data from the Torrents.

40. Mr Azima has brought separate proceedings against Mr Del Rosso and Vital in respect of the hacking in the US Federal Courts in North Carolina (where Mr Del Rosso and Vital are located).

C. THE PROJECT UPDATE

41. By about February 2015, RAKIA:

a. had used investigators to gather information on Mr Azima and others working with him;

b. had identified Mr Azima as an adversary.

42. In March 2015 Mr Page provided the Project Update to at least Mr Buchanan and Mr Gerrard, and briefed the Ruler on its contents.

43. A copy of the Project Update:

    a. accidentally survived RAKIA's and Mr Page's deliberate document destruction policy; and

    b. has been disclosed in very redacted form.

44. Mr Page:

    a. reported "[in] *continuation to our previous report*" that Mr Azima was managing a team in the US working for Dr Massaad to spread information about human rights abuses in RAK and that Dr Massaad had identified that Mr Gerrard was central to the cover up of those abuses. (The team also included Mr Kirby Behre, a US lawyer who had acted for Dr Massaad and Mr Azima; and Christopher Cooper, a PR consultant, both of whom were later also targeted, as described below);

    b. proposed taking action against Mr Azima and the "*US team*", including steps to "*gather intelligence on their progress in order to monitor their activities and attempt to contain or ruin their plans*".

45. In his witness statement for the First Trial, Mr Page:

    a. gave dishonest evidence that he had "*invariably*" reported to RAKIA orally and had first heard of Mr Azima in 2016;

    b. intentionally concealed the facts that:

        i. he was the author of the Project Update;

        ii. he had provided it to both Mr Buchanan and Mr Gerrard;

        iii. he reported to the Ruler and RAKIA, both orally and about half the time in writing, and had provided some 30 such reports over the course of his engagement;

        iv. he and RAKIA had operated a deliberate document destruction policy in order to keep those reports secret.

46. Witness statements for the First Trial were also provided by Mr Gerrard (two), Mr Buchanan (three) and the Ruler (one). As to these:

    a. Mr Gerrard's statements made no reference to the Project Update and suggested that Mr Gerrard had first encountered Mr Page in August 2016;

    b. Mr Buchanan's statements made no reference to the Project Update or to Mr Buchanan's dealings with Mr Page in 2015;

    c. The Ruler's witness statement made no reference to Mr Page and suggested that he was not aware of the Project Update or its contents.

47. It is to be inferred that:

    a. Each of Mr Page, Mr Gerrard, Mr Buchanan and the Ruler intentionally concealed the true facts about the Project Update and Mr Page's reporting to RAKIA.

    b. RAKIA and Mr Page intended to procure the obtaining of Mr Azima's confidential information including through hacking.

    c. Those proposals were acted on including by procuring the hacking.

D. THE RULER'S INSTRUCTIONS TO "TARGET" AND "GO AFTER" MR AZIMA

48. On or around 4 April 2015, the Ruler instructed Mr Buchanan to "*target*" Mr Azima.

49. Mr Buchanan discussed that instruction with Mr Handjani and Mr Naser Bustami (who sat on the board of RAK Development LLC), and Mr Bustami proposed that he, Mr Buchanan and Mr Handjani meet so as to "*hook up and coordinate our attack*".

50. On or around 19 July 2015, the Ruler instructed Mr Bustami to "*go after*" Mr Azima. Mr Bustami passed on that instruction to Mr Buchanan, who discussed it with Mr Handjani.

51. It is to be inferred that:

    a. the Ruler's instructions were prompted by the information conveyed in the Project Update and other such reports by Mr Page;

b. the Ruler's instructions were acted on by RAKIA's agents taking steps to procure the hacking of Mr Azima's data.

E. MALICIOUS EMAILS RECEIVED BY MR AZIMA AND OTHERS

52. A 'phishing' email is an email that seeks to trick the recipient into clicking on a malicious hyperlink or opening a malicious attachment and a 'spear-phishing' email is a 'phishing email' which targets specific individual(s) by including material specifically pertinent to the target.

53. At around the time of and in the months following the Project Update, Mr Azima and other persons associated with him and with Dr Massaad received a significant number of malicious emails including 'spear-phishing' and 'phishing' emails. Details of those of them which it has been possible to identify are set out in Schedule A.

54. The content, timing, provenance and other characteristics of these emails indicates that they (or a significant number of them) were sent as part of a single campaign targeting the recipients. Amongst other things:

a. Five emails with identical or very similar content were sent to Dr Massaad, Mr Azima, Mr Cooper and Dr Massaad's assistant (Ms Beudjekian) on 19-21 May 2015:

i. The emails included subject lines and contents referring to "Star Industrial Holdings Limited", which is a company owned by Dr Massaad.

ii. The same spoof sender email address is used in four of the five emails.

iii. The emails contained malicious links that sought to capture personal login details from the recipients.

b. There are numerous other instances in which the same spoof email address was used to send substantively identical malicious emails to multiple recipients within very short periods of time.

c. Mr Azima was targeted with phishing emails falsely purporting to be from family members, or business associates, including an email purporting to be from Ms Beudjekian.

d. Mr Behre was targeted with emails purporting to be from family or business associates.

e. Mr Behre received a series of emails beginning on 26 March 2015 (which is the date shown on the Project Update document).

f. Mr Azima received a series of emails beginning on 7 April 2015, several days after the Ruler's instruction to "*target*" Mr Azima.

g. Mr Azima received further emails in August 2015, following the Ruler's instruction to "*go after*" him.

h. Mr Cooper received dozens of emails in April and May 2015.

i. Emails were sent with false news regarding Mr Azima and Dr Massaad and their business operations.

j. Emails were sent to Mr Adams and Ms Azadeh (who were both employees of Mr Azima, who had dealings with RAKIA in 2015) falsely purporting to be from the other.

k. Identical or similar technical characteristics are present in the vast majority of the malicious emails. The nature of these characteristics will be addressed in expert evidence.

55. It is to be inferred that these emails were sent by persons acting on RAKIA's direct or indirect instructions (and/or on the instructions of one or more of the Additional Defendants, acting on behalf of RAKIA).

F. SUSPICIOUS ACCESS TO CERTAIN EMAIL ACCOUNTS

56. Mr Azima's email accounts were accessed on a number of occasions in 2015 and 2016 prior to the publication of the hacked material, including:

a. On multiple occasions between 13 and 15 October 2015, his account "fa@fa1.us", was accessed from IP addresses that are unfamiliar to Mr Azima;

b. Another account, "fa@farhadazima.com", was accessed from several countries with which Mr Azima had no connection, including India (in 2015) and Bulgaria (in around May 2016).

c. Unknown other instances including in regard to both these and other email accounts.

G. THE "VIEW FROM THE WINDOW" DOCUMENT

57. A document prepared by a consultant to RAKIA at the end of December 2015 (entitled '*View from the Window*') and sent by Mr Frank to Mr Gerrard on 4 January 2016 (approximately 7 months prior to the publication of the hacked material on the internet), stated that "*through a series of investigations*" it had been "*exposed as fact*" that, "*FA* [Mr Azima]*, a U.S. citizen, appears to have orchestrated, if not (fully) participated in numerous fraudulent activities*".

58. Mr Buchanan:

a. was the person within RAKIA leading the "RAK Project";

b. gave evidence at the First Trial that he had only believed Mr Azima to be involved in alleged fraudulent activities through sight of the hacked material, and claimed not to have seen the View from the Window document.

59. RAKIA, Mr Buchanan and Mr Gerrard have not explained where any alleged fraud had been "*exposed as fact*" other than through the hacked material.

60. It is to be inferred that:

a. RAKIA or its agents had by then obtained at least some access to Mr Azima's confidential data; and

b. that was the basis for the statements in the document.

H. THE RULER'S "WIDER OBJECTIVES"

61. On 2 March 2016, Mr Azima entered into a Settlement Agreement with RAKIA in regard to certain claims against RAKIA by HeavyLift International Airlines FZC ('**HeavyLift**'), a company owned by Mr Azima.

62. The Settlement Agreement was drafted by Mr Gerrard and/or Dechert, and included:

a. an express duty of good faith, binding on Mr Azima and HeavyLift, but not on RAKIA;

b. an English jurisdiction and choice of law clause.

63. Mr Buchanan and Mr Bustami recommended that the Ruler approve RAKIA entering into the Settlement Agreement and described the good faith clause as "*the key clause in this agreement bearing in mind your wider objectives*".

64. It is to be inferred that:

a. The "*wider objectives*" referred to were obtaining the means of attacking Mr Azima through litigation in London and associated publicity;

b. The good faith clause was key because it would enable RAKIA later to make damaging allegations against Mr Azima which would attract significant publicity (regardless of whether any claims were ultimately upheld);

c. RAKIA already believed at that stage that such claims might be possible, because it had by then already begun to obtain access to and analyse (at least some of) Mr Azima's data.

I. THE MEETING OF 16 JULY 2016

65. On 16 July 2016, a meeting was held between Mr Azima, Mr Buchanan, Mr Gerrard, and an associate in Mr Gerrard's firm, Dechert.

a. Prior to the meeting, and with Mr Buchanan's knowledge, Mr Gerrard had questioned Mr Azima on whether he had or had not acted in the interests of the Ruler, and referred to HeavyLift and Eurasia Hotel Holdings Limited (a company that had been incorporated on Mr Azima's instructions).

b. That exchange suggested that he had knowledge or suspicions about the conduct of those companies; which would be inconsistent with Mr Buchanan having only believed that Mr Azima had been involved in any alleged fraudulent activities upon seeing the hacked data unless they had already had some sight of that data.

c. At the meeting:

i. Mr Gerrard wanted Mr Azima to shift his alignment to assist RAKIA in its dispute with Dr Massaad;

ii. Mr Gerrard told Mr Azima that if he did not do so and Dr Massaad would not agree to a settlement, Mr Azima would be made "collateral damage" in the ensuing battle.

66. It is to be inferred that RAKIA. Mr Buchanan and Mr Gerrard by then had knowledge of Mr Azima's confidential data and anticipated that the data would be publicised and otherwise used by RAKIA against Mr Azima.

J. THE EMAILS "BREAKING THE NEWS"

67. On 15 August 2016, Mr Gerrard emailed Mr Del Rosso:

> *"I've had another call from Stuart who confirms again that there is a website on FA. He seems to think it's been generated from a UAE source. I've asked for details. He said he would try and get them to me. Can you undertake a search for it?"*

68. Mr Gerrard and Mr Del Rosso exchanged further emails on 15 and 16 August 2016 and Mr Gerrard stated that he would ask "*Stuart*" (ie, Mr Page) for further details and information.

69. On 16 August 2016, Mr Buchanan emailed Mr Frank and Mr Handjani, copying in Mr Gerrard:

> *"Good morning. I have been informed by Stuart last night that there is an internet site that is carrying a huge amount of material relating to FA - I will get you the link later. I have asked Neil to have a team start reviewing the material as a matter of urgency. At this time, I have no idea whether this relates to us or whether it is of value in respect of our ongoing dispute with KM. More importantly, I cannot tell you whether there is anything on the site about which we should have any concern. Clearly, it would be very interesting to know who is behind this action - Stuart tells me it is UAE based. We will speak later. Jamie"*

70. These emails suggest that the existence of the websites was first reported to RAKIA by Mr Page in and around 15 to 16 August 2016.

a. That suggestion is false because:

i. RAKIA's evidence at the First Trial was that Mr Gerrard and Mr Del Rosso, and Mr Buchanan and Mr Gerrard, had discussed the websites on 8 or 9 August 2016. Mr Gerrard gave evidence that he discussed the websites with Mr Del Rosso after being told about them by Mr Page.

ii. Mr Del Rosso, on Mr Gerrard's instruction, had already engaged NTi to download the data on 12 August 2016.

iii. Mr Page gave evidence that he only contacted Mr Gerrard once regarding the websites.

iv. Mr Gerrard did not seek details from Mr Page.

v. Mr Buchanan did not later send the link to Mr Frank or Mr Handjani.

vi. Mr Frank and Mr Handjani did not reply to Mr Buchanan.

vii. Mr Handjani gave evidence that he did not in 2016 know who "Stuart" was.

b. It is to be inferred that the emails were intentionally written to confect a documentary trail purporting to evidence the 'innocent discovery' of the Torrents.

K. THE TORRENTS

71. In August and September 2016, around 30 GB of Mr Azima's data appeared in three tranches on online anonymous peer-to-peer platforms known as torrents (the '**Torrents**').

a. The data included confidential, personal and private data accumulated over 10 years, and a substantial number of privileged communications.

b. The first tranche comprised data of around 27.775 GB and appeared on or around 4 August 2016.

c. The second tranche comprised data of around 10.33 MB and appeared on or around 30 August 2016.

d. The third tranche comprised data of around 4.43 GB and appeared on or around 8 September 2016.

72. The data

a. was obtained without Mr Azima's authorisation;

b. included emails taken from 10 email accounts belonging to Mr Azima and Mr Adams (the Chief Financial Officer of Heavylift):

i. *cfo@globalsubdive.com*

ii. *fa@alphaavia.com*

iii. *fa@fa1.us*

iv. *farhad@farhadazima.com*

v. *farhadazima@yahoo.com*

vi. *farhadusa@me.com*

vii. *fazima@gmail.com*

viii. *HH@fathers.church*

ix. *ray.adams@algkc.com*

x. *ray@jfjintl.com;*

c. included Mr Azima's appointments, call history, photos, recordings, SMS messages, Viber messages, videos, voicemails, WhatsApps, contacts and notes;

d. included around: (i) 161,702 emails; (ii) 13,736 photographs or other images; and (iii) 840 voice recordings.

e. included material of the most personal kind about Mr Azima and his family.

73. RAKIA:

a. accessed all 30 GB of data;

b. procured the publication of all of the data on the Torrents (including the personal material);

c. analysed the hacked material;

d. on 23 September 2016, represented by Dechert, sent a pre-action letter to Mr Azima's referring to various of Mr Azima's confidential documents and attaching some of them;

e. on 30 September 2016, commenced proceedings against Mr Azima relying on documents from the hacked material;

f. relied on the data in the First Trial.

74. In the course of First Trial, RAKIA's case as to how it obtained the hacked data and as to its knowledge of who created the Torrents:

a. Was first set out in a witness statement from its solicitor, Mr Hughes, on 13 July 2018 - that a public relations company which had been monitoring internet publications on its behalf discovered publicly available links to BitTorrent websites.

b. Was changed in pleadings signed on 6 November and 11 December 2018, which said that:

i. Mr Page had been informed of the existence on publicly available links of the first Torrent by Mr Majdi Halabi, and that Mr Page then informed Mr Gerrard of this, who informed Mr Buchanan;

ii. Mr Page later learned of publicly available links to the second Torrent, and informed Mr Gerrard of these.

75. That account was not supported by any documentary evidence at all, and there were significant inconsistencies in it, including the following:

a. Mr Halabi's evidence was that he had found two links to the first Torrent on one occasion which he then provided to Mr Page in a single communication. Mr Page's evidence was to the same effect. However, an email sent by Mr Del Rosso on 9 August 2016 stated that two websites had been identified at two different points in time;

b. The 15 and 16 August 2016 'breaking the news' emails referred to above are inconsistent with the email sent by Mr Del Rosso on 9 August 2016, and with Mr Page's evidence that he contacted Mr Gerrard about the websites only once;

c. While RAKIA said the materials were publicly accessible, they were not accessible when a contractor appointed by Mr Del Rosso to download it first attempted to do so (on and prior to 22 August 2016). The first Torrent only became allegedly accessible after NTi raised the difficulty with Mr Del Rosso;

d. The 'public accessibility' of the materials is contradicted by the fact that the materials subsequently could not be accessed by RAKIA's own expert in proceedings brought by Mr Azima in the United States.

76. The case RAKIA presented as to how it obtained the hacked data and as to its knowledge of who created the Torrents was:

a. untrue;

b. known by Mr Page and Mr Halabi to be untrue;

c. by inference (including in view of the matters set out below in respect of CyberRoot), known by Mr Buchanan, Mr Gerrard and Mr Del Rosso to be untrue;

d. through all of those individuals, known by RAKIA to be untrue.

L. CYBERROOT

77. Between 28 July 2015 and 22 September 2017, Vital made 35 payments totalling $1,018,046.39 to CyberRoot.

78. At least a substantial portion of those payments was for work performed for RAKIA, on the instructions of Mr Del Rosso, in turn instructed by Mr Gerrard and/or Dechert.

79. Gravitas also made substantial payments to CyberRoot in the same period, by inference on behalf of RAKIA.

80. CyberRoot is a 'hack-for-hire' firm and hacked Mr Azima's emails and devices on behalf of RAKIA. That conclusion is supported by the following facts:

a. An employee of Cyber Root, Preeti Thapliyal, was previously employed by BellTrox InfoTech Services ('***BellTrox***').

b. BellTrox has been publicly implicated in hacking. On 11 February 2015, the founder and owner of BellTrox, Sumit Gupta, was indicted by the United States in the Northern District of California for hacking. Mr. Gupta remains at large.

c. According to a June 9, 2020 press report by Thomson Reuters, BellTroX was involved in "*one of the largest spy-for-hire operations ever exposed*," helping clients spy on more than 10,000 email accounts over a period of seven years.

d. BellTrox and CyberRoot shared servers and hacking infrastructure.

e. Preeti Thapliyal has the technical capability to conduct hacking and has stated in her profile and CV that while at BellTrox she, "*Worked on Custom Build Phishing Campaigns Framework*", and "*Created undetectable phishing Payloads*". Prior to working at BellTrox, she stated that she "*Worked on a project of Hardware hacking using Rfid and Arduino*".

f. An employee of CyberRoot, Mr Vikash Kumar Pandey, admitted to an investigator acting for Mr Azima, Mr Jonas Rey - as was true - that:

i. CyberRoot was working to carry out hacking of Dr Massaad and Mr Azima by around June or July 2015.

ii. In around July 2015, CyberRoot gained access to certain of Dr Massaad's data.

iii. In around March/ April 2016, CyberRoot gained access to certain of Mr Azima's data.

iv. CyberRoot utilised infrastructure established by BellTrox to carry out this hacking.

g. The payments made by Vital on RAKIA's behalf to CyberRoot.

h. The payments made by Gravitas to CyberRoot.

M. THE DELETION OF MR BUCHANAN'S EMAILS

81. Mr Buchanan was RAKIA's primary disclosure custodian.

82. On 3 October 2016, Mr Azima's US lawyers sought assurances from Dechert that RAKIA had complied with its obligations to preserve documents. Dechert gave that assurance on 20 October 2016.

83. Upon giving disclosure on 25 April 2019, RAKIA for the first time informed Mr Azima's lawyers that a number of emails from Mr Buchanan's email account had allegedly been deleted on 12 October 2016 and allegedly could not be recovered.

84. The deletions were very substantial: For the First Trial:

a. Mr Azima disclosed 198 emails sent from Mr Buchanan to him. Only 1 of those emails apparently appears in the image RAKIA's lawyers have of the "sent" items folder of Mr Buchanan's account.

b. Mr Azima disclosed 106 emails that he sent to Mr Buchanan. Only 83 of these appear in the image of Mr Buchanan's inbox.

85. Mr Buchanan has claimed that the emails were mistakenly deleted by an Apple store employee without his permission when he attended the Apple store in London in October 2016.

86. It is to be inferred that this account is false and that Mr Buchanan deliberately destroyed emails (including emails between Mr Buchanan and other parties on RAKIA's side) in order to conceal evidence of wrongdoing:

a. It is highly unlikely that an Apple employee would delete substantial numbers of emails without a customer's permission.

b. RAKIA accepted that if there had been such a mistaken deletion it would not have affected any part of the inbox or its sub-folders. But around 20% of Mr Buchanan's inbox was missing (in addition to the 99% of his sent items folder).

c. Mr Buchanan had been asked about the preservation of his emails by RAKIA's solicitors in August 2017, and had not told them of any incident at the Apple store in October 2016.

d. No documents of any kind were disclosed by RAKIA that showed Mr Buchanan to have attended the Apple store.

e. Mr Buchanan belatedly said in oral evidence that he had been accompanied to the Apple store by a "witness" but has never identified that person.

N. MR GERRARD'S AND MR HUGHES' EVIDENCE AS TO DEALINGS WITH MR AL SADEQ

87. The Project Update refers to Mr Karam Al Sadeq, who was formerly the general counsel of RAKIA and was detained in RAK in around September 2014.

88. RAKIA alleged that Mr Azima had sought to spread false media stories regarding abuses against prisoners in RAK, including allegations that Dechert was involved in the mistreatment of prisoners.

89. The issues in the First Trial included whether allegations that prisoners were mistreated in RAK (and that Dechert was involved) were false.

90. In the First Trial Mr Gerrard gave evidence that:

a. he interviewed Mr Al Sadeq only once;

b. in interviewing Mr Al Sadeq, he had followed the requirements of the Police and Criminal Evidence Act ('**PACE'**), and/or had followed the requirements as closely as possible;

c. he only interviewed Mr Al Sadeq in the presence of Mr Al Sadeq's lawyer;

d. when interviewing Mr Al Sadeq, he was accompanied by other local lawyers, from the firm Al Tamimi;

e. he did not believe that he had interviewed Mrs Al Sadeq;

f. he did not believe that he had interviewed Mr Al Sadeq before he was charged;

g. he had interviewed Mr Al Sadeq in prison.

91. Following publication of the judgment, Mr Gerrard provided a belated "corrective witness statement" in which he admitted that:

a. he interviewed Mr Al Sadeq at least six times: four times in September and October 2014, once in August 2015, and once in April 2016; and had further 'meetings' with Mr Al Sadeq while Mr Al Sadeq was detained;

b. a process for interviewing prisoners resembling PACE had been put in place only in October 2015;

c. Mr Al Sadeq's lawyer was not present for any of the interviews conducted in 2014;

d. Al Tamimi did not attend any of the "at least" four interviews that occurred in 2014, or the interview in April 2016;

e. he met with Mrs Al Sadeq on a number of occasions, and that these included multiple occasions that could be regarded as interviews;

f. he interviewed Mr Al Sadeq in: (i) the RAK general police headquarters; (ii) a military prison; and (iii) the RAK central courthouse;

g. he did in fact interview Mr Al Sadeq before he was charged; and

h. he learned that Mr Al Sadeq was represented by a lawyer in 2015.

92. Mr Gerrard has since admitted that he was informed that Mr Al Sadeq had a lawyer on 23 September 2014 (before Mr Al Sadeq was interviewed in October 2014).

93. It is to be inferred that:

a. Mr Gerrard knowingly gave false evidence because he wished to minimise the suggestion that prisoners in RAK were improperly treated and to distance himself and Dechert from any allegation of mistreatment;

b. Mr Gerrard only filed his "corrective statement" because he was served with proceedings brought by Mr Al Sadeq against him, Mr Hughes, another Dechert solicitor (Ms Caroline Black), and Dechert, alleging their role in his mistreatment while in prison and realised that his false evidence might be exposed in those proceedings.

c. Mr Gerrard deliberately held back his 'corrective evidence' until judgment had been handed down.

94. *RAKIA v Bestfort Development LLP* (Claim No. HC-2015-003109) is another case in which the Defendants (adverse to RAKIA) complain of hacking. Mr Page was involved in obtaining investigative services for RAKIA; and RAKIA was represented by Mr David Hughes (previously of Dechert, but now of Stewarts, RAKIA's current solicitors).

a. In an application for an interim order pending an appeal, RAKIA relied upon a witness statement dated 3 December 2015 from Mr Hughes (then still a partner of Dechert) ('**8th Hughes**').

b. 8th Hughes purported to provide information to the Court of Appeal as to new developments in the investigation conducted by Dechert on RAKIA's behalf, and stated in paragraph 8:

> *"Furthermore, the Investigation is still ongoing and new information continues to be uncovered: for example, I carried out interviews on 8 October 2015 and 29 October 2015 with Mr Karam Al Sadeq, who*

was General Counsel of the First Appellant from November 2008 to November 2012, and Deputy CEO of the First Appellant to Dr Massaad from about June 2011 to November 2012. This was the first time that it has been possible to interview Mr Al Sadeq."

c. That evidence was false. Mr Al Sadeq had been interviewed repeatedly in September and October 2014, as well as in August 2015, and Mr Hughes was himself present at interrogations of Mr Al-Sadeq in October 2014.

d. It is to be inferred that Mr Hughes gave false evidence in order to serve RAKIA's interests, and that RAKIA and Mr Gerrard must have been party to him doing so.

O. MR PAGE'S THREAT TO "IMPLICATE" OTHERS

95. In August or September 2020, Mr Page told Mr Buchanan that "*if I have to implicate Nick / Patrick, Decherts, Neil and the boss to get me out of this I will.*" This statement referred to Mr Del Rosso ("*Nick*"), Mr Grayson ("*Patrick*"), Dechert, Mr Gerrard ("*Neil*") and the Ruler ("*the boss*").

96. Mr Page has admitted making that statement in correspondence, but suggested it was only referring to the possibility that he might identify the working relations of those individuals and their knowledge of each other. That is an implausible attempt to gloss the plain meaning of the word "implicate".

97. It is to be inferred that Mr Page has information showing those parties to be involved in wrongdoing, including attempts to obtain confidential information from Mr Al Sadeq's legal team and/or from Mr Azima and his associates.

P. FURTHER PUBLICATION ON WETRANSFER SITES

98. In addition to the Torrents, a large volume of data confidential to Mr Azima was disseminated on WeTransfer sites:

a. One dataset was made available on WeTransfer on 27 January 2017 (and deleted on or around 9 May 2019).

b. A further dataset was made available on WeTransfer on 3 June 2019, and remains available now.

99. Mr Pandey has admitted to Mr Rey (which is alleged to be true) that CyberRoot made these data available on WeTransfer. It is inferred that CyberRoot did so on instructions from Mr Del Rosso, Vital or another agent of RAKIA.

IV. THE HACKING OF MR AZIMA AND THE COVER UP OF THE FACTS RELATING TO IT

100. The established facts, and the inferences which fall to be drawn from all of the facts, are set out below.

101. Mr Azima's emails and computers were hacked on one or more occasions, by one or more parties.

102. Multiple individuals and entities were instructed to hack and disseminate Mr Azima's data or procure others to do so and may have acted either together or in parallel. At least:

a. Mr Page sought to engage hackers to attack Mr Azima in connection with his role in the "Project".

b. Mr Del Rosso engaged CyberRoot, to carry out hacking of Mr Azima (and Dr Massaad) and to disseminate Mr Azima's data.

103. Each of Mr Page and Mr Del Rosso did so as agents of RAKIA, and their knowledge and conduct is attributable to RAKIA.

104. Mr Buchanan paid CyberRoot for unknown services, on behalf of RAKIA. It is a reasonable inference that such apparent retainer by Mr Buchanan of CyberRoot was in furtherance of the conspiracy and unlawful acts of RAKIA against Mr Azima.

105. RAKIA:

a. procured the hacking of Mr Azima's emails and computers on one or more occasions;

b. procured the release of the Torrents so as to be able fraudulently to claim that it had found and accessed the hacked data innocently on the internet; and

c. subsequently sought to cover up the true facts in regard to the hacking;

d. is liable both primarily and vicariously for the acts of Mr Gerrard, Mr Page, Mr Del Rosso, Mr Buchanan and Mr Grayson.

106. That RAKIA did those things is supported by, in summary, the following matters of inference, circumstantial evidence and (in the case of the matters deposed to by Mr Rey set out herein) direct evidence (as set out in detail above):

a. RAKIA attempted to obtain information on Dr Massaad and Mr Azima through the "RAK Project".

b. RAKIA engaged several agents to carry out the "RAK Project", including Mr Page and Mr Grayson, who have been implicated in wrongdoing in other proceedings.

c. The Project Update.

d. RAKIA and Mr Page's document destruction policy.

e. The false evidence at the First Trial about the Project Update and similar reports and Mr Page's role.

f. The Ruler's instructions to "*target*" and "*go after*" Mr Azima.

g. The malicious email attacks on Mr Azima and other persons identified by RAKIA in the Project Update and their timing.

h. The fact that email accounts belonging to Mr Azima were accessed.

i. The internal record in December 2015 that it had been "*exposed as fact*" that Mr Azima had participated in fraud, when no such exposure at that time had been demonstrated.

j. RAKIA's 'wider objectives' in entering into the Settlement Agreement included to bind Mr Azima to a wide-ranging and one-sided duty of good faith, accompanied by an English jurisdiction clause.

k. Mr Gerrard's threat in July 2016 that Mr Azima would be rendered 'collateral damage'.

l. The Torrents emerged very shortly after settlement talks with Dr Massaad collapsed.

m. RAKIA advanced an untrue explanation for the discovery of the Torrents.

n. Mr Gerrard and Mr Buchanan sent deceptive emails purporting to 'break the news' of the Torrents.

o. Mr Del Rosso engaged CyberRoot on behalf of RAKIA and Vital was instrumental in paying it over $1m.

p. Mr Buchanan (through Gravitas) also made material payments to CyberRoot.

q. CyberRoot successfully hacked Mr Azima.

r. CyberRoot established the Torrents.

s. Mr Buchanan intentionally deleted a significant number of his emails and concocted a false cover story.

t. Mr Gerrard and Mr Hughes have both given false evidence as to their interviews with Mr Al Sadeq.

u. Mr Page has stated that he will "*implicate*" Mr Gerrard, Dechert, the Ruler, and Mr Del Rosso, as well as Mr Grayson.

v. RAKIA's concealment and cover up of the true facts.

w. No party other than RAKIA has sought to use the hacked materials in proceedings against Mr Azima.

107. Mr Page (as set out in detail above):

a. was closely involved in the "RAK Project", and made the proposal to "*gather intelligence on their* [ie, the US team managed by Mr Azima] *progress in order to monitor their activities and attempt to contain or ruin their plans*";

b. was party to a deliberate document destruction policy as to his work for RAKIA and RAK;

c. gave false evidence at the First Trial as to:

i. his role in the 'Project Update';

ii. his knowledge of Mr Azima before 2016;

iii. his explanations for his false evidence on those matters;

iv. his supposed 'innocent discovery' of the Torrents;

d. has been found in other proceedings to have links to hackers and has been implicated in other serious wrongdoing;

e. has stated that he would "*implicate*" Mr Gerrard, Dechert, Mr Del Rosso, the Ruler and Mr Grayson in wrongdoing;

f. received significant remuneration for his work for RAKIA;

g. has been identified by an unnamed source to an investigator as having sought assistance with hacking Mr Azima from as early as October 2014;

h. by inference was party to the hacking, the staged release of the data and the cover up.

108. Mr Buchanan (as set out in detail above):

a. was the leading figure in RAKIA's investigations, including the 'RAK Project';

b. instructed both Mr Page and Mr Gerrard;

c. was instructed by the Ruler to "*target*" and "*go after*" Mr Azima and discussed implementing those instructions with other individuals on RAKIA's side;

d. briefed the Ruler that RAKIA's "wider objectives" in entering into the Settlement Agreement in March 2016 were to bind Mr Azima to a wide-ranging and one-sided duty of good faith;

e. attended the meeting on 16 July 2016 at which Mr Gerrard threatened Mr Azima;

f. through Gravitas made substantial payments to CyberRoot;

g. was privy to Mr Page's wrongful activities and party to the false evidence about them at the First Trial;

h. was party to the false version advanced in the First Trial as to the discovery of the Torrents;

i. was party to the staged 'breaking the news' emails;

j. deleted a significant number of emails in order to conceal his and RAKIA's complicity in the hacking, and concocted a false cover story;

k. by inference, was party to the hacking, the staged release of the data and the cover up.

109. Mr Gerrard:

a. was closely involved in the 'RAK Project' and RAKIA's investigations and was both party to and involved in the development of its strategy in regard to Mr Azima at all material times;

b. gave instructions to Mr Page and was privy to his wrongful activities, and was party to the false evidence about them at the First Trial;

c. gave instructions to Mr Del Rosso and Vital to engage CyberRoot, by inference to procure the hacking;

d. was party to the staged 'breaking the news' emails;

e. was party to the false version advanced in the First Trial as to the discovery of the Torrents;

f. was the recipient of the '*View from the Window*' document;

g. threatened Mr Azima on 16 July 2016, shortly before the release of the hacked data, that he would be rendered "collateral damage" if he did not switch sides to assist RAKIA and a settlement was not reached;

h. has been identified by Mr Page as someone he will implicate;

i. gave false evidence as to his involvement with Mr Al Sadeq, and was party to Mr Hughes doing so;

j. by inference, was party to the hacking, the staged release of the data and the cover up.

110. Mr Gerrard's knowledge and conduct is to be attributed to Dechert; and/or Dechert is vicariously liable for Mr Gerrard's acts.

V. PROPER LAW

111. RAKIA has agreed in clause 7 of the Settlement Agreement that English law will apply in respect of it and that the courts of England and Wales have exclusive jurisdiction in respect of the same matters. The US Court of Appeals has determined that the scope of matters covered by this clause includes Mr Azima's complaints of hacking against RAKIA. Mr Azima's claims against RAKIA arising out of the above facts are accordingly subject to English law.

112. The proper law applicable to Mr Azima's claims against Dechert, Mr Gerrard, Mr Buchanan and Mr Page arising out of the hacking is the Federal law of the United States of America and the State law of the State of Missouri:

a. Pursuant to The Law Applicable to Contractual Obligations and Non-Contractual Obligations (Amendment etc.) (EU Exit) Regulations 2019 (the EU Exit Regulations) and subject to the amendments in article 11 of those Regulations, the Rome II Regulation EU 864/2007 ("Rome II") remains applicable in the United Kingdom as Retained EU Law.

b. Pursuant to article 4 of Rome II,

> *"(1) Unless otherwise provided for in this Regulation, the law applicable to a non-contractual obligation arising out of a tort/delict shall be the law of the country in which the damage occurs irrespective of the country in which the event giving rise to the damage occurred and irrespective of the country or countries in which the indirect consequences of that event occur.*
>
> *(2) However, where the person claimed to be liable and the person sustaining damage both have their habitual residence in the same country at the time when the damage occurs, the law of that country shall apply.*
>
> *(3) Where it is clear from all the circumstances of the case that the tort/delict is manifestly more closely connected with a country other than that indicated in paragraphs 1 or 2, the law of that other country shall apply. A manifestly closer connection with another country might be based in particular on a pre-existing relationship between the parties, such as a contract, that is closely connected with the tort/delict in question."*

c. Each of the claims arising from the hacking addressed below are claims "*arising out of a tort/delict*" within the meaning of article 4(1).

d. The damage suffered by Mr Azima occurred internationally upon the publication of the hacked data, but was most directly suffered in Missouri because that was at the time the state in which Mr Azima permanently resided and from which he conducted business.

113. Alternatively, and in any event, the United States of America is the country, and the State of Missouri is the state, to which the torts or delicts are most closely connected, in that:

a. At the time of the hacking Mr Azima resided in and conducted business from Missouri.

b. Mr Azima's electronic devices which were hacked were ordinarily physically stored in Missouri.

c. Mr Azima ordinarily accessed the data which was ultimately hacked in Missouri.

d. The damage suffered by Mr Azima occurred internationally upon the publication of the hacked data, but was most directly suffered in Missouri because that was at the time the state in which Mr Azima permanently resided and from which he conducted business.

114. Alternatively,

a. the claims against all of the Defendants are subject to English law in consequence of the choice of law in the Settlement Agreement, and the fact that the Additional Defendants were acting as agents of RAKIA; or, further alternatively,

b. the claims against RAKIA (as well as the other Defendants) are subject to US Federal law and the State law of the State of Missouri for the reasons given in the previous paragraphs.

115. References to the Defendants collectively in setting out each of the claims below should in each case be read as references to the Defendants in regard to whom the claims are subject to English law, or US and Missouri law, as the case may be.

VI. MR AZIMA'S CLAIMS

A. CLAIMS UNDER ENGLISH LAW

1. Claims for unauthorised access, hacking, and theft of data

116. The relevant provisions of the Data Protection Act 1998 ("DPA") continue to have effect notwithstanding its repeal in 2018, pursuant to the Data Protection Act 2018, Schedule 20, paragraph 6.

117. Section 5 of the DPA established territorial limitations on its application. Those limitations are inapplicable and/or RAKIA waived or is estopped from relying on those limitations by reason of having agreed that English law would govern its relations with Mr Azima, as set out above.

118. The unauthorised access to Mr Azima's computers and emails, the hacking and theft of his data, and the disclosure on websites and other uses made by the Defendants of Mr Azima's stolen data constituted breaches of the DPA, actionable by Mr Azima against them. In particular:

a. The data RAKIA and the other Defendants obtained as a result of its hacking of Mr Azima's devices constitutes "data" under section 1(1) of the DPA. The hacking made each of the Defendants a "data controller" under that section, alternatively a "data processor".

b. As data controllers and data processors of Mr Azima's data, the Defendants had a duty under s4(4) to comply with the data protection principles in relation to all personal data obtained by their hacking.

c. Disclosure of Mr Azima's data online and the use of Mr Azima's data in pursuit of a campaign against him was a breach of the data protection principles in Schedule I, Part l of the DPA and specifically the principles that personal data be "processed fairly and lawfully" and that it be obtained "only for one or more specified and lawful purposes".

d. The Defendants are accordingly jointly and severally obliged under section 13 of the DPA, to compensate Mr Azima for all resulting losses, including damages

for both pecuniary and non-pecuniary loss and damages for distress occasioned by the breach.

e. Mr Azima is also entitled to an injunction to restrain further publication of his personal data obtained as a result of the hacking.

119. Further and/or alternatively, to the application of the DPA, the Computer Misuse Act 1990 ("CMA") applies as follows. The CMA establishes territorial limitations on the provisions imposing duties. Those limitations are inapplicable and/or RAKIA waived or is estopped from relying on those limitations by reason of having agreed that English law would govern its relations with Mr Azima, as set out above.

120. The unauthorised access to Mr Azima's computers and emails and the hacking and theft of his data was contrary to section 1 of the CMA:

a. This breach of statutory duty is actionable by Mr Azima.

b. The breach has caused Mr Azima loss and damage, as set out below.

c. The Defendants are therefore liable to pay damages.

2. Breach of Confidence and/ or Misuse of Private Information

121. The information obtained through the hacking (or a substantial part of it):

a. was private and confidential to Mr Azima;

b. was of a nature such that Mr Azima had a reasonable expectation of privacy in respect of its contents;

c. had the necessary quality of confidence, such that any person obtaining the information without authorisation would come under a duty of confidentiality in respect of it.

122. RAKIA and the Additional Defendants were responsible for the hacking, and thereby infringed Mr Azima's reasonable expectation of privacy.

123. Further, RAKIA and the Additional Defendants were under an obligation of confidence with respect to the information from the moment of its acquisition.

124. The publication of the information on internet sources, its distribution and/or unauthorised use in (and in connection with) the proceedings before this Court infringed

Mr Azima's reasonable expectation of privacy, and the obligation that these parties had to respect the confidence of the information.

125. These acts have caused serious detriment to Mr Azima.

126. In the premises, the acquisition of the information through the hacking, and/or the publication and misuse by RAKIA of the information obtained through the hacking was a misuse of and/or unjustified publication of private information and/ or a breach of confidence.

127. Mr Azima is therefore entitled to:

a. compensation for the financial loss and damage incurred in consequence upon the breach of confidence and/ or misuse of private information;

b. damages for the lost right to control private information and for the distress Mr Azima justifiably felt because his private information had been released into the public domain;

c. disgorgement of any gains accruing to any of the Defendants from their breach of confidence. The nature of these gains is not yet fully known, but will be particularised further if and when proper information and/or disclosure is provided.

3. Conspiracy to injure

128. In the circumstances described above, RAKIA and the other Defendants (with or without others) entered into a combination and an agreed course of conduct, with the predominant intention of harming Mr Azima.

129. The combination was covert and the full details are not known to Mr Azima, but it is alleged (without limitation) that it was formed and/or furthered:

a. when RAKIA instructed the Additional Defendants (separately or together) and Vital and Mr Del Rosso and through them CyberRoot to take steps to obtain Mr Azima's private information and to ensure that it became accessible on the internet;

b. by the proposal in the Project Update to "*gather intelligence*";

c. by the Ruler's instructions in April and July 2015 to target Mr Azima and the (undisclosed) communications which it can be inferred would have followed acting on those instructions.

130. The parties to the conspiracy put it into effect by:

a. procuring the hacking;

b. procuring the publication of Mr Azima's data on the internet;

c. procuring or promoting the websites drawing attention to the exposure of his private and confidential information;

d. thereafter, seeking to conceal and cover up such unlawful behaviour.

131. This conspiracy caused significant harm to Mr Azima and his business interests.

132. In the premises, the Defendants are liable to Mr Azima for damages for conspiracy to injure.

4. Unlawful Means Conspiracy

133. In addition, and in any event, each of the acts in furtherance of the conspiracy (alternatively, some of them) was unlawful:

a. Hacking is unlawful under criminal law in England and Wales, as well as in the United States and Missouri. It is also a civil wrong, as set out above and below.

b. The publication of Mr Azima's data is unlawful: (i) in England and Wales as a breach of confidence and/or a misuse of private information; and (ii) in the United States and Missouri as set out below;

c. The procuring and promoting of websites is unlawful as a further or aggravated infringement of Mr Azima's privacy and/or disclosure of his private information and/or interference with his business interests.

d. The concealment and cover up of the hacking was unlawful as it involved the giving of false evidence.

134. Each of the Defendants knew, or were reckless to the fact, that their acts in furtherance of the conspiracy were unlawful.

135. This unlawful conspiracy caused significant harm to Mr Azima and his business interests.

136. In the premises, the Defendants are liable to Mr Azima for damages for unlawful means conspiracy

B. CLAIMS UNDER US FEDERAL LAW AND MISSOURI LAW

137. As a result of their conduct described above, each of the Defendants are liable to Mr Azima under United States Federal Law and under Missouri Law for the losses which he has suffered particularised below; under one or more of the following causes of action.

1. Conspiracy to Disclose and Use Intercepted Wire, Oral, or Electronic Communications under the Wiretap Act (18 U.S.C. §§ 2511(1)(d) and 2520, 18 U.S.C. § 371; and Disclosure and Use of Wire, Oral, or Electronic Communications under the Wiretap Act (18 U.S.C. §§ 2511(1)(c) and 2520)

138. Each of the Defendants:

a. knowingly agreed and conspired with each other and with CyberRoot and others to intercept Mr Azima's data by hacking and to disclose Mr Azima's intercepted data in violation of 18 U.S.C. §§ 2511 and 2520; and

b. each of the Defendants took steps in furtherance of the conspiracy.

139. It is a violation of 18 U.S.C. § 2511(c) for any person intentionally to disclose, or to make endeavours to disclose, to any other person the contents of any electronic communication, knowing or having reason to know that the information was obtained through the interception of electronic communication, where:

a. "*Intercep*t" is defined as *"the .. acquisition of the contents of any .. electronic .. communication through the use of any electronic, mechanical, or other device*." 18 U.S.C. § 2510(4); and

b. "*Electronic communication*" means "*any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce*."

140. The Defendants intercepted Mr Azima's data by the hacking of his computers and email accounts and obtaining persistent, real-time access to Mr Azima's accounts. The persistent access gave the Defendants immediate and contemporaneous copies of Mr Azima's emails in real-time.

141. The Defendants disclosed and endeavoured to disclose Mr Azima's data by publishing the intercepted data on the Torrents. Defendants added new links to Mr Azima's data multiple times and as recently as June 2019.

142. The Defendants used and endeavoured to use the hacked data against Mr Azima including to damage him (and conspired in doing so).

143. By being party to the hacking and the dissemination of Mr Azima's data the Defendants knew or had reason to know that the data had been intercepted from Mr Azima.

144. As a result of the conspiracy and the disclosure of Azima's intercepted data, Mr Azima suffered damage.

145. Since at least June 2018, the stolen data has continued to be publicly available on WeTransfer through links that were created on the instructions of the Defendants (or some of them), resulting in damage to Mr Azima.

2. Misappropriation of Trade Secrets, 18 U.S.C. §§ 1831, 1832, 1836

146. In US Federal law:

a. The Defense of Trade Secrets Act creates a cause of action against *"[w]hoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly . . . steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains*" trade secrets. 18 U.S.C. § 1832(a)(1).

b. "*An owner of a trade secret that is misappropriated may bring a civil action . . . if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce*." 18 U.S.C. § 1836(b)(1).

147. Mr Azima's email accounts and computer systems stored trade secrets intended for use in interstate and foreign commerce, including but not limited to highly confidential

business plans and proposals, research supporting those plans and proposals (including costs and service projections), information concerning business strategies and opportunities, and contacts for important business relationships.

148. The Defendants unlawfully conspired:

a. to take, appropriate, and obtain Azima's trade secrets without authorization, by means of a cyberattack against him, knowing that Azima's email accounts contained trade secrets and intending to steal them in order to harm Azima.

b. to disseminate those trade secrets and to continue to do so including as recently as June 2019.

149. As a result of the conspiracy and hacking Mr Azima has suffered damage, which includes, but is not limited to, loss of business goodwill, loss in the value of his trade secrets and confidential business information, and harm to Mr Azima's business.

3. The United States Computer Fraud and Abuse Act

150. Under the United States Computer Fraud and Abuse Act ("CFAA"), I 8 U.S.C. § 1030,§ 1030, prohibitions and civil remedies are created for unauthorised access to computers in certain circumstances:

a. The CFAA designates as "*protected computers*" computers *" used in or affecting interstate or international commerce*": as defined by 18 U.S.C. § l030(e)(2)(8).

b. Mr Azima's computers were at all material times "*protected computers*" as so defined.

c. The CFAA prohibits a person from intentionally accessing a protected computer without authorisation and thereby obtaining information from that protected computer: 18 U.S.C. § 1030(a)(2)(C).

d. RAKIA and the other Defendants or persons acting on their behalf knowingly and intentionally accessed Mr Azima's devices without Mr Azima's authorisation, thereby obtaining around 30GB of Mr Azima's data unlawfully.

e. In the premises, RAKIA's hacking was a breach of 18 U.S.C. § 1030(a)(2)(C).

151. It is also contrary to the CFAA intentionally to access a protected computer without authorization, and as a result of such conduct, recklessly cause damage: 18 U.S.C. §l030(a)(5)(B).

a. The hacking of Mr Azima's devices enabled the Defendants to alter Mr Azima's data, contrary to this provision.

b. The CFAA provides a right to a civil remedy to recover damages including for loss: 18 U.S.C. §1030(e)(11).

152. As a direct consequence of the hacking, Mr Azima was forced to dispose of and replace the computers infected as part of the hacking, and his business was disrupted.

153. The Defendants thereby recklessly caused damage in violation of 18 U.S.C. §1030(a)(5)(B): and caused damage and actionable loss (as defined by 18 U.S.C. § 1030(e)(11) to Mr Azima in violation of§ 1030(a)(5)(C); and are therefore liable to Mr Azima under the CFAA.

4. The Missouri Computer Tampering Act ("MCTA")

154. In terms of section 569.095.1, a person who undertakes "*computer tampering*" includes a person who:

> *"knowingly and without authorization or without reasonable grounds to believe that he or she has such authorization: ..*
>
> *(3) Discloses or takes data, programs, or supporting documentation, residing or existing internal or external to a computer, computer system, or computer network; or*
>
> *(4) Discloses or takes a password, identifying code, personal identification number, or other confidential information about a computer system or network that is intended to or does control access to the computer system or network; or*
>
> *(5) Accesses a computer, a computer system, or a computer network, and intentionally examines information about another person; or*
>
> *(6) Receives, retains, uses, or discloses any data he or she knows or believes was obtained in violation of this subsection."*

155. In terms of section 537.525 of the Revised Statutes of Missouri, Tampering with Computer Data, Computer Equipment or Computer Users Act, the owner of a computer system, computer network, or data, that has been tampered with is entitled to recover compensatory damages, including expenditures reasonably and necessary incurred to verify that a system, network, or data was not altered, damaged, or deleted by the access

156. The hacking amounted to computer tampering within the meaning of the MCTA.

157. Each of the Defendants were party to the computer tampering, and are therefore jointly and severally liable to Mr Azima for compensatory damages, including expenditures reasonably and necessary incurred to verify that a system, network, or data was not altered, damaged, or deleted by the access.

5. Invasion of Privacy Torts – Intrusion on the Seclusion of Another

158. By being party to the hacking, each of the Defendants:

a. intentionally intruded on the solitude, seclusion, or private affairs of Mr Azima;

b. by a means that is unreasonable or highly offensive to a reasonable person in that:

i. the hacked data included secret and private subject matter;

ii. that the plaintiff had the right to keep secret; and

iii. which the defendants obtained in an unreasonable way.

159. In consequence the Defendants are jointly and severally liable for damages for intrusion into his interest in privacy, for mental distress suffered through invasion of privacy, and for special damages.

6. Invasion of Privacy - Public Disclosure of Private Facts

160. By being party to the hacking and dissemination of Mr Azima's data, each of the Defendants was party to:

a. publication to a large number of persons;

b. without waiver or privilege;

c. of private matters in which the public had no legitimate concern; and

d. in such a way as to bring shame or humiliation to an individual of ordinary sensibilities.

161. In consequence the Defendants are jointly and severally liable for damages for harm to his interest in privacy, for mental distress suffered through invasion of privacy, and for the specific damages caused by their disclosure.

7. Tortious Interference with Business Relationship and Business Expectancy

162. Each of the defendants knew that Mr Azima conducted business as described above and had a valid expectancy of continuing to do so.

163. By being party to the hacking and dissemination of Mr Azima's data, the Defendants:

a. intentionally interfered with Mr Azima's business and business expectancy;

b. by the employment of improper means,

c. causing the severance of business relationships and loss of business expectancy;

d. in circumstances in which the defendants had no legal right to interfere,

e. resulting in damage as particularised below.

8. Conspiracy

164. By being party to the hacking and dissemination of Mr Azima's data, each of the defendants was party to a civil conspiracy under Missouri law:

a. The defendants had a meeting of minds as to the pursuit of the unlawful hacking and the dissemination of the data; and

b. Each committed at least one act in furtherance of the conspiracy; and

c. The plaintiff was thereby damaged.

C. LOSS, DAMAGE AND OTHER RELIEF

1. Pecuniary Losses

165. By reason of the above wrongs, Mr Azima has suffered loss and damage for which RAKIA is liable to pay compensation.

166. As a result of the hacking Mr Azima required professional assistance to investigate it and was forced to dispose of his previous devices and to purchase new ones, and as a result suffered the following damages:

a. Cost or professional services required (from ZP Consultants LLC) to investigate and mitigate the hacking, $183,000.

b. Replacement of 4 computers, $17,274

c. Protective software for 5 years, $18,784.

167. In addition, Mr Azima suffered extensive damage to his business. Mr Azima is unable to particularise those damages pending:

a. the application for permission to appeal to the Supreme Court, and (if permission is granted) the appeal; and

b. the determination of the full extent of such hacking and the parties involved therein and/or its explanation by RAKIA.

2. Non-Pecuniary Losses

168. The publication of Mr Azima's private information and data caused substantial distress and emotional harm. A significant award is necessary to compensate for the distress and for the gross invasion of his privacy, in addition to damages to compensate for his pecuniary losses pleaded above.

3. Exemplary Damages

169. The hacking was deliberate, and was procured by a State-sponsored entity deliberately in order to inflict damage on Mr Azima, on the cynical basis that he would (even if he could prove his complaint) be unable to be do anything to obtain compensation which

would effectively remedy that damage including his resulting personal distress, or would deprive RAKIA of what it gained from the hacking of Mr Azima.

170. In those circumstances, RAKIA should be liable for exemplary damages.

4. Disgorgement

171. It is to be inferred that the Defendants (or some of them) accrued gains from their invasion of Mr Azima's privacy and breach of his confidence, including in the form of fees for the provisions of their services.

172. Mr Azima is therefore entitled to an order requiring that each of the Defendants account to Mr Azima for all financial gains made as a result of the invasion of his privacy and breach of his confidence.

5. Interest

173. The Defendant is entitled to and claims interest on all compensation recovered pursuant to Section 35A of the Senior Courts Act l981.

6. Injunctive Relief

174. In addition to the damages claimed, Mr Azima is entitled to and claims injunctive relief against RAKIA and the other Defendants to restrain their continuing wrongs and the ongoing breach of his rights. Mr Azima seeks an injunction requiring RAKlA and/or all of the Defendants:

a. to take all reasonable steps to remove or procure the removal of the websites, torrents, WeTransfer links or other internet sources containing statements about Mr Azima, and/or providing means for his private data to be accessed by others;

b. to deliver up and/or destroy all copies of his private data in their or their agents' possession;

c. to disclose the full extent of such hacking and the parties involved therein including pursuant to the *Norwich Pharmacal* jurisdiction so that Mr Azima may vindicate his rights as against any such additional wrongdoers.

TIM LORD Q.C.

THOMAS PLEWMAN Q.C.

HUGO LEITH

Statement of truth

I believe that the facts stated in this Amended Counterclaim and Claim against Additional Defendants are true. I understand that proceedings for contempt of court may be brought against anyone who makes, or causes to be made, a false statement in a document verified by a statement of truth without an honest belief in its truth.

Signed: ……..

Date: [____] 2021

Name: Farhad Azima